

Celia Nogales  
Federal Regulatory Relations

1275 Pennsylvania Avenue, N.W., Suite 1801  
Washington, D.C. 20004  
(202) 383 6423

PACIFIC  TELESIS  
Group - Washington

January 14, 1994

RECEIVED

JAN 14 1994

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

William F. Caton  
Acting Secretary  
Federal Communications Commission  
Mail Stop 1170  
1919 M Street, N.W., Room 222  
Washington, D.C. 20554

Dear Mr. Caton:

Re: CC Docket No. 93-292 } *Policies and Rules Concerning Toll Fraud*

On behalf of Pacific Bell and Nevada Bell, please find enclosed an original and six copies of their "Comments" in the above proceeding.

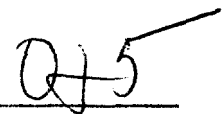
Please stamp and return the provided copy to confirm your receipt. Please contact me should you have any questions or require additional information concerning this matter.

Sincerely,

 /ksp

Enclosures

No. of Copies rec'd  
List A B C D E



Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

RECEIVED

JAN 14 1994

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

In the Matter of )

Policies and Rules )

Concerning Toll Fraud )

CC Docket No. 93-292

COMMENTS OF PACIFIC BELL AND NEVADA BELL

JAMES P. TUTHILL  
NANCY C. WOOLF

140 New Montgomery St., Rm. 1523  
San Francisco, California 94105  
(415) 542-7657

JAMES L. WURTZ

1275 Pennsylvania Avenue, N.W.  
Washington, D.C. 20004  
(202) 383-6472

Attorneys for Pacific Bell  
and Nevada Bell

Date: January 14, 1994

## TABLE OF CONTENTS

	<u>Page</u>
SUMMARY .....	iii
COMMENTS OF PACIFIC BELL AND NEVADA BELL .....	1
I. INTRODUCTION .....	1
A. Many Industry Efforts Are Underway To Combat Toll Fraud .....	1
B. Prevention Is Key To Combatting Toll Fraud ..	2
C. The Pacific Companies Have An Established, Successful Fraud Protection Program .....	4
D. Liability Must Be Commensurate With Control And Business Risk .....	8
II. PBX (REMOTE ACCESS) FRAUD .....	10
A. LECs Should Not Bear Responsibility For Remote Access Fraud .....	11
III. PAYPHONE FRAUD .....	13
A. Blocking And Screening Do Not Always Prevent Fraud .....	13
B. The Florida Rules Are Too Broad And Do Not Reflect The Realities Of Toll Fraud .....	15
IV. LIDB FRAUD .....	16
A. To Minimize Fraud, We Must Receive Adequate Information From Other Carriers .....	16
B. LECs' Tariff Liability Limitation Must Be Upheld .....	18

TABLE OF CONTENTS  
(Cont'd)

	<u>Page</u>
V. COORDINATION AND LAW ENFORCEMENT .....	19
A. Prosecution Of Toll Fraud Offenders Has Not Been Successful .....	19
VI. PART 68 CHANGES .....	21
VII. INCENTIVES .....	21
CONCLUSION .....	22

## SUMMARY

Organized toll fraud is a major problem, affecting nearly all members of the telecommunications industry. The Pacific Companies have been dedicated to trying to understand, prevent, detect, and intervene to stop toll fraud. We also have tried to prosecute offenders. Of all of these efforts, prevention is the key. If adequate controls are in place, and customers are warned and educated, toll fraud opportunities will be minimized.

Every party should be doing what it can to prevent and minimize toll fraud. Because of the changing methods used by toll fraud perpetrators, however, toll fraud will be difficult to eliminate. As safeguards are developed, new forms of fraudulent conduct appear. Nevertheless, each industry participant should be upholding minimum standards to minimize the possibility of toll fraud.

Our Centralized Fraud Bureau monitors every switch in our network to detect patterns that indicate toll fraud, and we take action to intervene and stop the fraud from continuing. Pacific Bell has instituted an education program which trains customers and employees in prevention and early warning signs of toll fraud. Pacific Bell is also in the process of issuing a comprehensive handbook on remote access fraud prevention. These efforts have made a difference; our per incident dollar loss is 1/10 the national average.

Liability for toll fraud must be commensurate with a party's ability to prevent the fraud from occurring. Liability must also be based upon the party's business reward. So, for example, if parties fail to take actions which would have prevented the fraud, they should be liable for the consequences. And, if no one is "at fault," but fraud still occurs, the party who would normally reap the business reward should shoulder most of the liability.

JAN 11 1994

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

In the Matter of )

Policies and Rules )  
Concerning Toll Fraud )

CC Docket No. 93-292

COMMENTS OF PACIFIC BELL AND NEVADA BELL

Pacific Bell and Nevada Bell (the "Pacific Companies") file these comments in response to the Notice of Proposed Rulemaking released December 2, 1993 ("NPRM"). We support the Commission's interest in this widespread problem, but urge the Commission to impose liability only on parties who have the ability to control or prevent the fraud. The Commission should also support the industry in designing technological solutions to known methods of toll fraud, and in prosecuting fraud perpetrators.

I. INTRODUCTION

A. Many Industry Efforts Are Underway To Combat Toll Fraud

Organized toll fraud is pervasive. It typically involves "call-sell" operations where fraud perpetrators invade privately owned CPE and then use that equipment to place unauthorized calls; use compromised calling cards or other alternate billing services (collect, billed-to-third

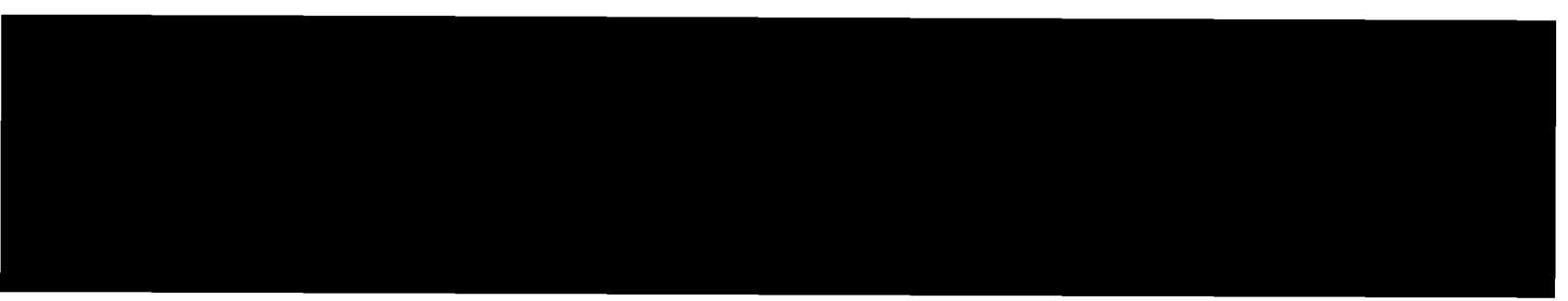
calls) to complete fraudulent calls; or establish service with no intent to pay the bills.<sup>1</sup> These methods of organized fraud are not mutually exclusive. For example, a "call-sell" operation using remote access fraud or a compromised calling card can be operated from a location where service has been established with no intent to pay the bill. Similarly, remote access and calling card fraud can be operated from pay telephones.

There are many efforts underway to combat toll fraud. We have deployed network monitoring programs which can detect fraud early so that we can intervene to stop fraudulent activity. Pacific Bell is also active in educating customers to the dangers of toll fraud.

The industry has responded by setting up a Toll Fraud Prevention Committee ("TFPC"), a subgroup of the Network Operations Forum of Alliance for Telecommunications Industry Solutions ("ATIS", formerly the Exchange Carriers Standards Association ("ECSA")). Pacific Bell also participates in the California Toll Fraud Task Force. The purposes of these groups are to identify toll fraud and design prevention techniques.

#### B. Prevention Is Key To Combatting Toll Fraud

Attacking toll fraud consists of prevention, detection, intervention and prosecution. The most important





of these is prevention. If prevention measures are in place and effective, detection, intervention, prosecution and liability issues are less important. For that reason, prevention should be the key focus for combatting toll fraud.

Prevention includes educating and warning customers about toll fraud, and establishing minimum standards that telecommunications industry participants must meet. The national TFPC has issued two position papers addressing toll fraud: one dealing with subscription fraud, and the other with fraud in telecom systems. These papers suggest minimum standards each player in the industry should meet to prevent and detect toll fraud. Because these suggestions were issued without regard for the implementation costs, they need to be reexamined by the industry. Even so, the Commission can use these papers as a starting point for determining the responsibilities of each industry participant. Copies of these two position papers are attached hereto as Exhibit A.

Preventing all toll fraud is impossible. As technology changes to prevent one type of toll fraud, the fraud perpetrators switch to some other method. However, there are some common "tools" perpetrators frequently need and use to commit their crimes. These "tools" include (1) inadequately secured PBX and CPE equipment with unprotected maintenance ports, direct inward dialing capabilities, voice mail, or auto-attendants; (2) a public

payphone with unrestricted alternate billing and international calling capabilities; (3) a residence or business phone with custom calling features such as 3-way calling, call waiting, call forwarding international - programmable and/or unrestricted alternate billing and international calling capabilities; and (4) inability of LECs and IXC's to adequately verify or validate the true identification of the subscriber.

If the industry and the Commission could design adequate safeguards for these tools, toll fraud could be minimized. Such an effort must be industry-wide, must have input from all affected parties and must be mandated by the Commission to get appropriate attention. The position papers issued by the TFPC are a good attempt to start this process for safeguarding the telephone network.

C. The Pacific Companies Have An Established, Successful Fraud Protection Program

We have various structures in place to minimize toll fraud losses. We have developed an adjunct to LIDB which contains a state-of-the-art fraud detection system, Pacific Bell Sleuth. In addition, our Data Base Administration Centers provide advice to hundreds of customers per day, including notification of suspected fraudulent use of their calling card, and measures customers can take to prevent compromise of their card. In addition, in 1992, in order to reduce losses associated with organized

"call-sell" fraud, Pacific Bell established a Centralized Fraud Bureau to detect, intervene and prevent subscription and remote access fraud.<sup>2</sup>

In order to detect fraud more rapidly, we have developed an enhanced detection program which monitors every switch in our network and has reduced the time in which we can detect fraudulent activity from approximately three days to as early as six to twelve hours. The network surveillance system is able to rapidly detect known fraudulent "call-sell" patterns. We also receive early-warning referrals from LIDB on alternately billed calls. These processes have enabled us to detect and stop over 500 cases of organized fraud each month, preventing approximately \$3 million per month in fraudulent "call-sell" loss revenue.

In addition to detecting the fraud faster, the Centralized Fraud Bureau has set up an aggressive intervention process. This process includes notifying the customer as soon as the fraud is detected, and working on the problem until resolution. This work may include speaking with the vendor of the customer premises equipment to provide information based on our past experience of how the fraud may be occurring.

Pacific Bell does far more than just notify a customer. Pacific Bell has been authorized by the

---

<sup>2</sup> The Centralized Fraud Bureau also handles surveillance of calls in Nevada Bell's territory.

California Public Utilities Commission, via an 18-month provisional fraud tariff, to disconnect service without advance written notice in cases where documented organized call-sell subscription fraud can be determined.<sup>3</sup> This tariff is vital to minimize the losses associated with call-sell subscription fraud.

In addition to the early detection and intervention outlined above, Pacific Bell has been a leader in the industry in trying to prevent toll fraud. Pacific Bell's fraud prevention service, known as Pacific Bell LockOn<sup>SM</sup> Toll Fraud Protection Services, provides the customer with a number of educational services including 1) awareness training to customers and employees, 2) customer premises risk assessments, 3) publication of materials outlining the different types of fraud and how customers can prevent it, 4) a hotline to report suspected fraud, and 5) a handbook that explains in detail the different types of (CPE-based) toll fraud, what the customer can do to prevent fraud, and what we are doing to prevent, detect and intervene in toll fraud cases. The handbook, which will be available to customers at the end of January, provides ten pages of checklists that customers can use to ensure that their particular CPE is as secure as possible. Attached as Exhibit B is a copy of the handbook. Pacific Bell provides all of these services at no charge to the customer.

---

<sup>3</sup> Schedule Cal.P.U.C. NO. A2.1.11.A.5.

In recognition of these efforts in preventing toll fraud, Telecom Network & Security Review has named Pacific Bell as the "LEC of the year" for its work against toll fraud.

The Commission has asked for comment on the efficacy of education programs, monitoring, fraud detection equipment, etc.<sup>4</sup> The problem with toll fraud prevention is that it is not static. As the carriers and PBX vendors find ways to prevent toll fraud, fraud perpetrators find ways around the systems in place. Nonetheless, our fraud monitoring and detection systems have made a substantial reduction in toll fraud.

For example, we have been the first to detect the fraud and notify the customer in 60% of the incidents. This figure is increasing as our programs and monitoring systems are enhanced. Also, our statistics show that our Centralized Fraud Bureau handled 17 cases of remote access fraud in March 1993. In November, we handled 48 cases of remote access fraud. Despite the increase in cases handled by the Fraud Bureau, the average revenue at risk in each incident is quite low. The national average for remote access toll fraud is \$125,000 per incident.<sup>5</sup> The average within the Pacific Companies is \$10,000 per incident, a testament to our early detection of fraudulent activities.

---

<sup>4</sup> NPRM, para. 26.

<sup>5</sup> Telecom & Network Security Review, March 1993, at 7.

D. Liability Must Be Commensurate With Control And Business Risk

Throughout this NPRM the Commission has sought comment on how liability should be assigned in various types of toll fraud.<sup>6</sup> Because toll fraud is continually changing -- fraud perpetrators change their operations as technology changes -- hard and fast rules are difficult to apply. Also, every player in the industry has different business needs, goals and incentives. What is achievable for one carrier may not be possible for another.

Liability must be commensurate with prevention and reward. All industry participants have responsibility for different parts of the network and the services provided. The industry participants reaping the business reward should bear the business risk if fraud occurs. For example, for remote access fraud, the control over the CPE is generally with the business owner, who can institute protections or disable the remote access. If the business owner decides to use the remote access feature despite the risk, then that business owner must accept the consequences.

Similarly, for customer-owned payphones (COPT), we automatically restrict international calling when the line is provisioned. COPT providers can choose to unblock this restriction, but if they do, they must bear responsibility for international calls.

---

<sup>6</sup> See, for example, NPRM, paras. 24, 25, 31, 39.

As a LIDB owner, we have some control over the validation of our calling card. However, we are limited in our control by the incomplete information given to us by other network providers. Therefore, these other providers should share in the risk of toll fraud. For an international call, for example, the business reward is mostly with the long distance carrier. That carrier should legitimately bear most of the risk.

Business risk and reward is also important to review when determining liability for toll fraud. LECs can only carry calls intraLATA. For access, we simply provide the first, or last, leg of the call's journey, and are compensated for it regardless of the destination of the call.

Risk must follow reward. It is clear that international calls account for the bulk of toll fraud calls. However, LECs don't play in the international market, other than as access providers. The LEC network is involved only briefly at the start of an international call. For a typical toll fraud call originating in California and destined for the Dominican Republic, our network is used for only the first few miles of the call. The average access charge is about 2 cents per minute.<sup>7</sup> The more lucrative long distance charges for international calling go to the IXC. Requiring us to participate in liability for the

---

<sup>7</sup> Assuming the call is FGD with average mileage of 10 miles.

entirety of the call would be akin to holding a taxi driver who takes a customer to the airport responsible when that customer hijacks an airplane.

When both the ability to control the fraud and the business risks and rewards flowing to the different industry participants are examined, some guidelines can be determined for liability. In the next sections of these comments, we will describe the different types of fraud in more detail and our recommendations for determining liability.

## II. PBX (REMOTE ACCESS) FRAUD

Organized remote access fraud consists of gaining access to privately-owned CPE, and then using that equipment to place unauthorized calls. The fraudulent calls can originate at any type of phone, private or payphone. The CPE subject to the fraud may be a customer-owned switch, a PBX, voice mail system, auto attendant or automatic call diverter.

For a business with a PBX, the remote access feature allows employees who are off premises to dial into the PBX and access all capabilities, including long distance service. This feature is often used in connection with 800 service. If a company is not using this feature, then the company can disable it. Companies that want to use this PBX feature must take into account the dangers of remote access fraud and avail themselves of the protections available.



The Commission requests comment on how liability should be imposed, what responsibilities the carriers have, and what other preventive measures parties might take.<sup>8</sup> As stated earlier, Pacific Bell currently has an array of education, detection and intervention processes in place. Because control over remote access fraud is with the PBX or business owner, we do not support any increased liability on the part of LECs.

A. LECs Should Not Bear Responsibility For Remote Access Fraud

The LEC involvement in PBX fraud is minimal. For a PBX, the LEC provides only the PBX trunks going from the PBX on the customer's premises to the central office. This trunk is a pipe only; there are no features or functionality associated with it. All of the features and functionality are in the CPE. Therefore, the controls are in the hands of the business owner.

The Commission has requested comment on how liability should be apportioned for PBX fraud.<sup>9</sup> Because the LEC has no control over the features or functions enabled or disabled within the PBX equipment, and because the LEC simply offers access to the network without more, the LEC should not bear any responsibility for customers who are subjected to PBX fraud.

---

<sup>8</sup> NPRM, paras. 24, 25, 26.

<sup>9</sup> NPRM, para. 25.

We do not believe that the Commission should engage in an instance-by-instance comparative negligence resolution in each case of toll fraud.<sup>10</sup> Neither carriers nor the Commission have resources for this effort. Instead, the Commission should set forth guidelines of parties' responsibilities for telecommunications fraud prevention. If all measures are taken by each party and toll fraud still occurs, then the responsibility should be with the customer, under the general rule that a customer is responsible for all calls made from its equipment. The Commission correctly determined in Chartways that a PBX owner is liable for fraud from its equipment.<sup>11</sup>

The Commission has tentatively concluded that tariff liability provisions that fail to recognize a duty by the carrier to warn customers of risks of using carrier services are unreasonable.<sup>12</sup> While our tariffs do not specifically set out this obligation, our activities with the Centralized Fraud Bureau, the LockOn<sup>sm</sup> Toll Fraud Protection Service, and aggressive education and training programs certainly satisfy the obligation to warn customers of these risks. Again, we have taken on this responsibility despite the fact that we have no control over PBX equipment

---

<sup>10</sup> NPRM, para. 25.

<sup>11</sup> 8 FCC Rcd 5601 (1993). See also, AT&T v. Jiffy Lube Int'l., 818 F. Supp. 1164 (D. Md. 1993) (holding the carrier's customer responsible for long distance calls made through its telephone system).

<sup>12</sup> NPRM, paras. 24, 26

and the vast majority of toll fraud calls are not local, but international.

### III. PAYPHONE FRAUD

The Commission has requested comment on the availability of Originating Line Screening ("OLS") and Billed Number Screening ("BNS") to payphone providers. The Commission also seeks comment on whether to adopt the Florida approach, which releases a payphone provider from liability for charges resulting from certain types of fraudulent calls if the provider purchases call screening.<sup>13</sup>

#### A. Blocking And Screening Do Not Always Prevent Fraud

The Commission has asked for comment on the availability of blocking and screening services for payphone providers.<sup>14</sup> In our territories, we provide COPT providers with OLS and BNS<sup>15</sup> on every COPT line at no additional charge. We also provide international direct dial

---

<sup>13</sup> NPRM, paras. 27-31.

<sup>14</sup> NPRM, para 31.

<sup>15</sup> OLS provides a notification to the operator service provider that the call originates from a payphone. BNS protect against the payphone being used as the recipient of collect or billed-to-third calls.

blocking.<sup>16</sup> OLS and BNS are therefore present on every line associated with a payphone. These blocking and screening functions are effective in preventing fraud, although there are limitations in their use, many of which are beyond the LEC's control.

For example, a screen code which is placed in the digit stream for OLS may not be received by an operator service provider or IXC unless its equipment is programmed to receive it. Thus, no action may be taken as a result of a screen code. Or, a COPT provider may order BNS so that no collect or billed-to-third calls are placed to the payphone. However, if the carrier at the originating location chooses not to validate a call through LIDB, BNS is ineffective and fraudulent calls can go through.

Also, if a customer requests a long distance operator to transfer it to another carrier's operator, the screen codes are normally not transferred with the call, which may allow fraudulent calls to get into the network. Holding the LEC responsible for fraud in these circumstances would not be equitable, and would not follow the general rule of risk following reward.

The Commission could assist in the process by having the industry devise technology based solutions to some blocking functions. The industry needs cooperative

---

<sup>16</sup> For COPT lines, international direct dial blocking is part of the service provisioned. A customer can request that we unblock this feature. For COPT-coin lines, international direct dial blocking will be provided, upon request, for no additional charge.

efforts at a high level to address the need to notify the carrier carrying the call that the originating number has been identified as a high risk for "call-sell" operations. This would give the carriers the information needed to monitor for fraudulent activity and to make a decision whether or not to process the call.

B. The Florida Rules Are Too Broad And Do Not Reflect The Realities Of Toll Fraud

The Commission has asked for comment on whether to adopt the Florida approach to payphone provider liability for toll fraud.<sup>17</sup> A payphone can be involved in many types of fraud. "Call-sell" operations using remote access fraud, or alternate billing fraud (calling card, collect, or billed-to-third) can originate there. The set can also be used for organized fraud where the payphone is the termination point for collect or billed to third fraud, clip on fraud (where the line is physically invaded and the set is bypassed), 10XXX-1+ fraud types, or set failure (where the payphone station suffers a failure that allows fraud to occur).

The Florida rules insulate the payphone provider from liability for 10XXX-1+, 10XXX-0+, 950-XXXX-0+, and 1-800 access code calling, as long as the provider has purchased OLS and BNS. However, as shown above, OLS and BNS are not always successful in preventing fraud. Certain

---

<sup>17</sup> NPRM, para. 31.

types of fraud are within the ability of a payphone provider to prevent. For example, we provide international direct dial blocking on every COPT line. A COPT provider can order that restriction to be removed, though. When providers decide that they do not want that protection, they should not be excused from toll fraud liability when fraudulent international calls are made from their payphone.

#### IV. LIDB FRAUD<sup>18</sup>

The Commission seeks comment on whether carriers querying a LIDB should provide carriers with calling and called party numbers, and how absence of this information affects the allocation of liability for toll losses.<sup>19</sup>

##### A. To Minimize Fraud, We Must Receive Adequate Information From Other Carriers

In order to enable our customers to use their calling cards from any phone at any time, we have a great interest in detecting and minimizing fraud on all networks. We have just completed the first phase of a multi-million dollar, multi-year program, Pacific Bell Sleuth, to enhance our fraud analysis system. When both calling and called numbers are provided, our ability to differentiate between a

---

<sup>18</sup> Since LIDB is simply a database that houses information, this section should really be entitled "Alternative Billing Services Fraud" since the organized fraud is associated with calling card, collect, and billed-to-third calls.

<sup>19</sup> NPRM, para 37.

fraudulent and a valid use calling pattern is substantially upgraded, and we can therefore detect fraud much quicker. In many cases today, carriers making LIDB queries do not provide us with calling and called number fields, or else they populate those fields with arbitrary numbers; this restricts our detection methods to simple threshold limit alerts.

When threshold limit alerts are the sole basis of fraud detection, many calling cards or billing numbers being used for legitimate high-volume calling are needlessly blocked, resulting in lost revenue and creating many customer service problems. We strongly support a Commission requirement that LIDB users provide originating station type, the originating calling party number, and called number in the LIDB query. When those numbers are provided to us, our fraud detection can move beyond threshold limits, and take full advantage of our new fraud detection system which looks at unique calling activity that may fit more sophisticated combinations of suspected fraudulent patterns. Without calling and called numbers, we cannot move to this higher level of detection with which we are equipping our network.

A more fundamental necessity not addressed by the Commission in the NPRM is the mandatory use of LIDB. In order to detect fraud, a carrier must use LIDB to validate each call. Some carriers do not validate while other carriers validate only some of the time. Without complete

information, our Pacific Bell Sleuth system is hampered in its ability to detect fraud. Therefore, a Commission directive requiring every carrier to query LIDB for each LEC joint use calling card or alternately billed call on a per call basis, and to provide originating station type, calling, and called numbers, would greatly enhance our fraud detection capabilities.

B. LECs' Tariff Liability Limitation Must Be Upheld

Limitations of liability clauses in the LEC tariffs are appropriate for LIDB use. Because of the importance of keeping our card competitive, we have spent and are planning to spend millions of dollars to enhance our fraud detection capabilities. However, those efforts are only as good as the data we receive and the cooperation between networks. To the extent that a carrier chooses not to query LIDB, or does not give us complete information, we should not share in the liability for toll fraud losses.

We do not believe that a blanket rule for allocating liability for toll losses can be made. Currently, carriers differ in technical capability to provide call processing information, early warning detection, speed of referral to the card issuer of suspected fraud, and other tools necessary for excellent fraud detection. Also, individual carriers have different views of the value of other network calling card acceptance and the risk and revenue impact for that carrier. Because of



the differences in the various players within the telecommunications industry, a uniform allocation rule would be extremely difficult to formulate. Instead, Pacific Bell is currently working with IXCs to negotiate mutual liability agreements based on shared capabilities and revenue opportunities. The Commission should continue to allow us this flexibility.

#### V. COORDINATION AND LAW ENFORCEMENT

The Commission seeks comment on how to achieve closer and continuing coordination among institutions fighting toll fraud. The Commission also seeks comment on what it can do to encourage appropriate law enforcement of toll fraud.<sup>20</sup>

##### A. Prosecution Of Toll Fraud Offenders Has Not Been Successful

We have been frustrated in our efforts to prosecute toll fraud criminals. At the federal level, there is a very high threshold minimum loss that must be met before an agency will even investigate a case. Even if an agency accepts the case, it is usually given low priority.<sup>21</sup>

---

<sup>20</sup> NPRM, para. 13.

<sup>21</sup> The primary federal agency investigating these offenses is the Secret Service. Because its highest priority is "personal protection" of the President and other dignitaries, toll fraud cases routinely get put aside for that more important work.